75th MORSS CD Cover Page

712CD

For office use only 41205

UNCLASSIFIED DISCLOSURE FORM CD Presentation

12-14 June 2007, at US Naval Academy, Annapolis, MD

Please complete this form 712CD as your cover page to your electronic briefing submission to the MORSS CD. Do not fax to the MORS office.

Author Request (To be completed by applicant) - The following author(s) request authority to disclose the following presentation in the MORSS Final Report, for inclusion on the MORSS CD and/or posting on the MORS web site.

Name of Principal Author and all other author(s): **A. Shaw, R. Mills, B. Mullins, and K. Hopkinson**

Principal Author's Organization and address:

R.F. Mills
Air Force Institute of Technology
AFIT/ENG
2950 Hobson Way
Wright-Patterson AFB OH 45433

Phone: **937-255-3636 x4527**

Fax:

Email: **robert.mills@afit.edu**

Original title on 712 A/B: **A Multilayer Graph Approach to Correlating Network Events with Operational Mission Impact**

Revised title: no change

Presented in (input and Bold one): (**WG 6/8**, CG___, Special Session ___, Poster, Demo, or Tutorial):

This presentation is believed to be:
UNCLASSIFIED AND APPROVED FOR PUBLIC RELEASE

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 JUL 2008	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A Multilayer Graph Approach to Correlating Network Events with Operational Mission Impact	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Institute of Technology AFIT/ENG Wright-Patterson AFB, OH 45433**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM202526. Military Operations Research Society Symposium (75th) Held in Annapolis, Maryland on June 12-14, 2007, The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**28**	

Air Force Institute of Technology

U.S. AIR FORCE

A Multilayer Graph Approach to Correlating Network Events with Operational Mission Impact

Al Shaw
Robert Mills
Barry Mullins
Kenneth Hopkinson

Center for Cyberspace Research
Air Force Institute of Technology
robert.mills@afit.edu

Educating the Future Leaders of America's Armed Forces

Overview

- The research problem
- Objectives
- Approach
- Completed and ongoing research
- Future research

The Problem

- Provide automated support in detecting computer network outages and degradations
  - Not enough to know there's a problem…need to know the effect on the customer's mission
  - Often called the "holy grail" of network management
- Current methods for this type of problem are mostly manual in nature
  - Network management tools focus on the network rather than the mission
  - First indications of mission impact are when people start calling the help desk
  - Even when we know there's an outage, it's difficult to explain the "so what?" factor to the commander

Limitations of Current NMS Technology

- Network Management Technology Survey
  - Network Auto-Discovery, Service Auto-Discovery
  - Correlation & Root-cause analysis techniques
  - Traffic Flow Analysis, Independent Agent Systems
  - Host-based Intrusion detection, Artificial Immune Systems
  - Active Networks

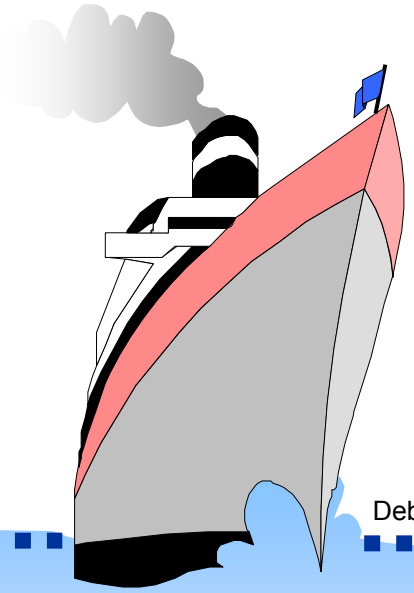
- Observations
  - NMS technologies allow increased visibility and control but cannot relate network status to mission capabilities
  - This information is simply not present in the network

Why Is This Important?

- If we can't do this now, how will we do it when everyone and everything is networked into the GIG?
- Increased Reliance on IT Raises Stakes for IT Service Providers
  - E-Business and E-Commerce
  - Network Centric Warfare
  - Capabilities that are enabled by IT resources
  - Is there any other kind??
- Bottom line: we need to know what kind of info is traversing the network

The Problem

Currently no automated way to tie IT status to the mission



Customers

IT Providers

IT-enabled Capabilities

Debra Curtis, Gartner Group 2004

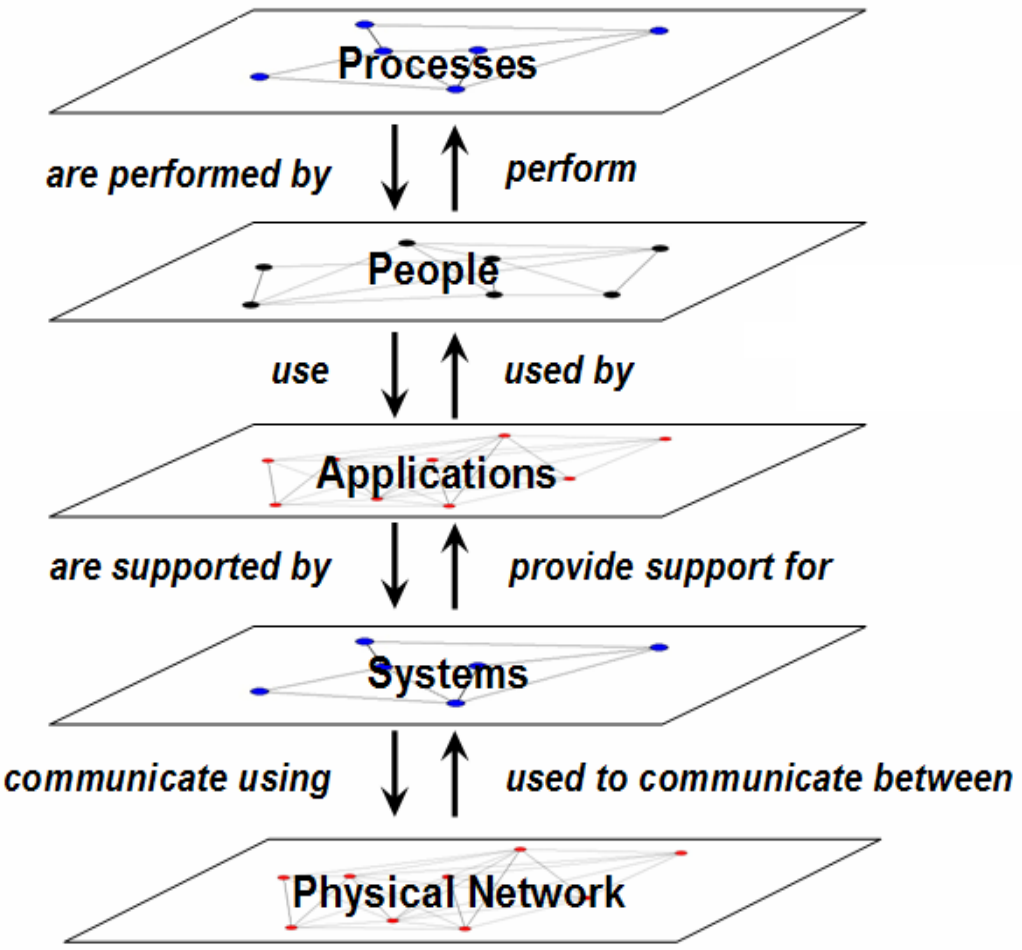
Traditional Network Management focused "below the water-line"

Mission Impact Analysis…need to automate link between IT and mission

Research Goals

- Framework for establishing traceability between systems, processes, and operational tasks and missions
  - Compatible with existing COP and DoD products
  - Practical, feasible, maintainable, complete, usable and accurate…
  - Self awareness, autopopulating
- Extensible
  - Build a cyberspace common operational picture

Multi-Layer Model for Net Centric Operations



Need clear mapping of cyber assets to physical world missions, tasks, organizations, etc.

Approach

- DoD Architecture Framework (DODAF)
  - Guidance for developing / presenting architecture descriptions
  - Used in describing DoD systems and processes
- Operational View (OV)
  - Business process modeling
  - Operational tasks and activities, information flows
  - Organizational relationships
- Systems View (SV)
  - Physical entities that make up an architecture
  - Computer systems, networks & system functions
  - Data exchanges and communication paths
  - Link systems to capabilities

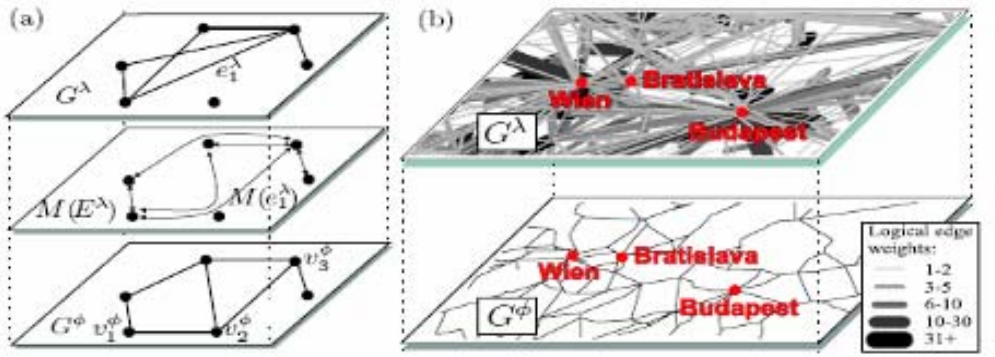
Approach

- Use multi-layer graph model based on DODAF
  - Mission View
  - Operational View
  - Systems View
- Linkages between layers establish traceability
  - Top down – facilitates comm planning and targeting
  - Bottom up – facilitates response and attack mitigation

Layered Complex Networks

- Marciej Kurant and Patrick Thiran, "*Layered Complex Networks*"
- Used to study complex systems
  - Multi-layered
  - Accounts for the interactions between and dependencies between physical and logical layers
- The two-layer model with the mapping $M(E_1^{\lambda})$ of the logical graph G^{λ} on the physical graph G^{Φ}. The logical edge e_1^{λ} is mapped on G^{Φ} as the path $M(E_1^{\lambda})=(v_1^{\Phi}, v_2^{\Phi}, v_3^{\Phi})$

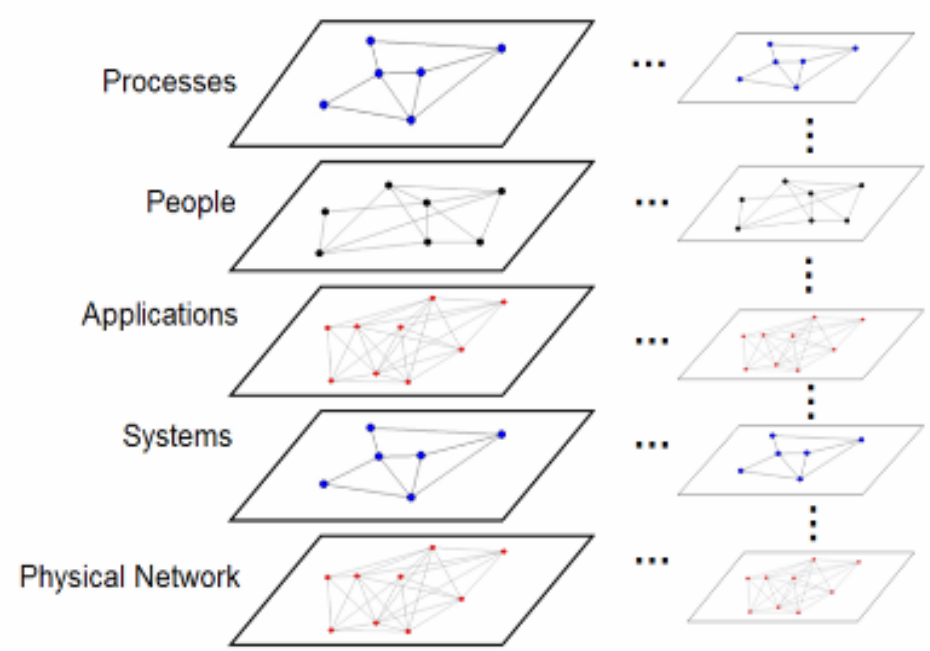
- "Logical" Layer = City Pairs
- "Traffic Route" Mapping = Route through Stations
- "Physical" Layer = Train Stations



Method for Incorporating Structure of the Underlying Network

Multi-Layer Model of NCO

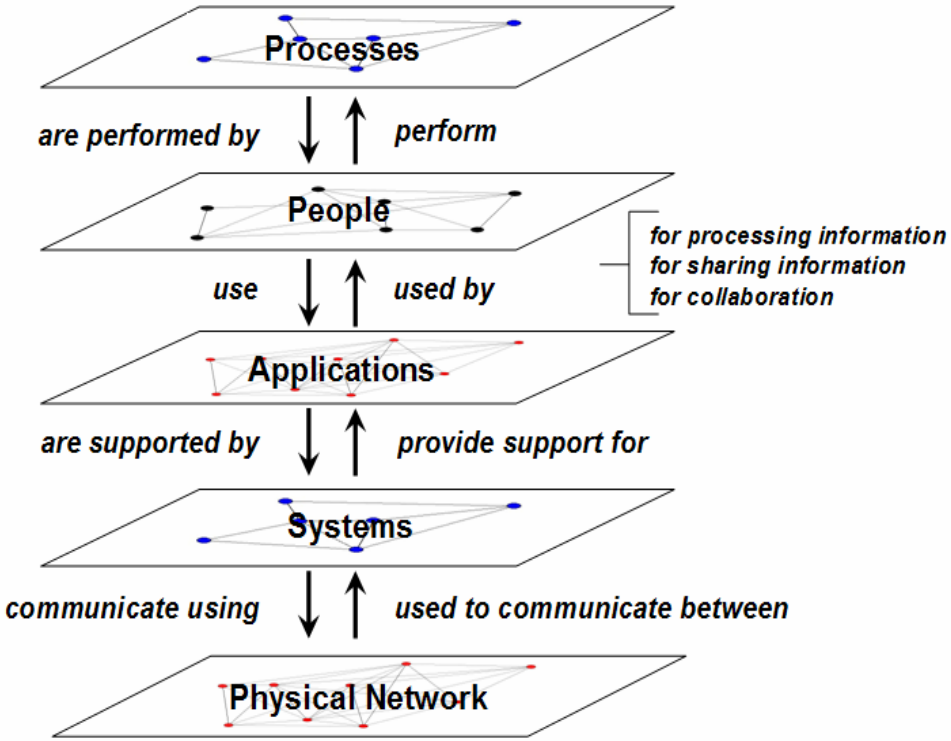
- Wong-Jiru – 2006
- Net Centric Operations represent complex systems with many different interacting elements
  - To measure net centricity, the complexity and interactive nature of NCO must be modeled
- Multi-layer model of NCO
  - Each layer represents major contributors to NCO
  - Relationships are graphically represented
  - Node and Edge definitions tailored to each layer



Layer	Node	Edge
Process	**Task**	**Transition**
People	**Position**	**Information path, working relationship**
Application	**Application**	**Data-specific Interoperability**
System	**Application support node/platform**	**Communication Interoperability**
Physical Network	**Infrastructure entities**	**Communication pathways, wired or wireless**

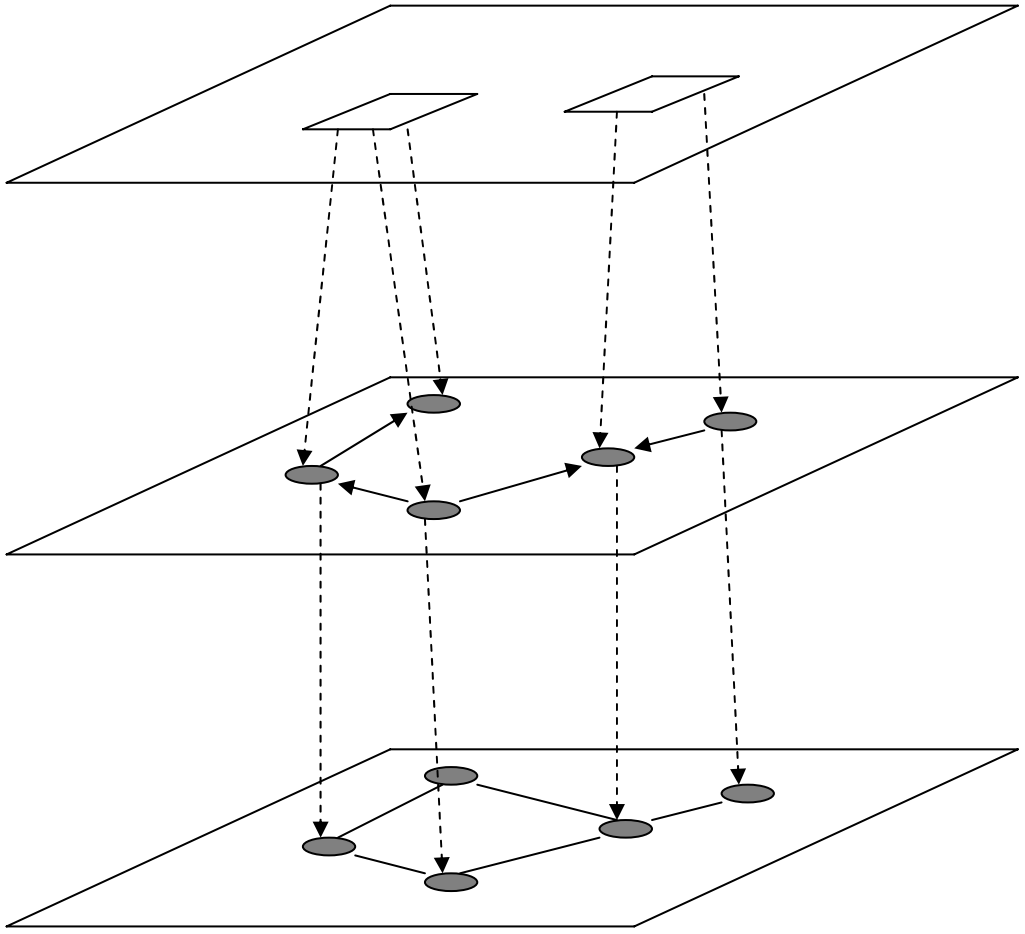
Multi-Layer Model of NCO: Interlayer Relationships

- Layers interact with each other
- Any failures or successes that occur at the lower layers may contribute (negatively or positively) upon the completion of mission objectives
- Interlayer relationships represented by *mappings*



Mapping	Node to Node Mapping	Edge to Edge Mapping
Process-People	Allocates task to people	Order or route of process tasks through people
People-Applications	Identifies the applications used by people	Route of information transactions through applications
Applications -Systems	Identifies which systems support which applications. For some, the system and application are the same	Route of information from application to application through supporting systems
Systems-Physical Network	Identifies which entry points into the communications infrastructure is accessed by which system	Route of communications from one system to another.

Air Operations Center Model



Mission Layer
-Mission
-METL

OV Layer
-Organizations
-Operational Nodes
-Tasks
-Informational Needlines

SV Layer
-Systems/Servers
-Networks/Links
-Functions
-Data Exchange Requirements

Information Tables

METL
Mission: Task Available Capabilities Description: Air missions are scheduled to be flown on a specific day. Accomplished through the ATO production process.

Mission Essential Tasks	
OP 2.1.1	Determine and prioritize operational priority intelligence requirements.
OP 2.1.3	Prepare operational collection plan.
OP 2.1.4	Allocate intelligence resources in the joint operations area.
OP 2.2.4	Determine logistical capability of the joint operations area.
OP 3.1.2	Apportion joint/multinational operational firepower resources.
OP 3.1.5	Publish air tasking order(s).
OP 6.1.1	Process/allocate operational aerospace targets.
OP 6.1.3	Provide airspace control.
ST 4.3.1	Establish and coordinate movement services within theater.

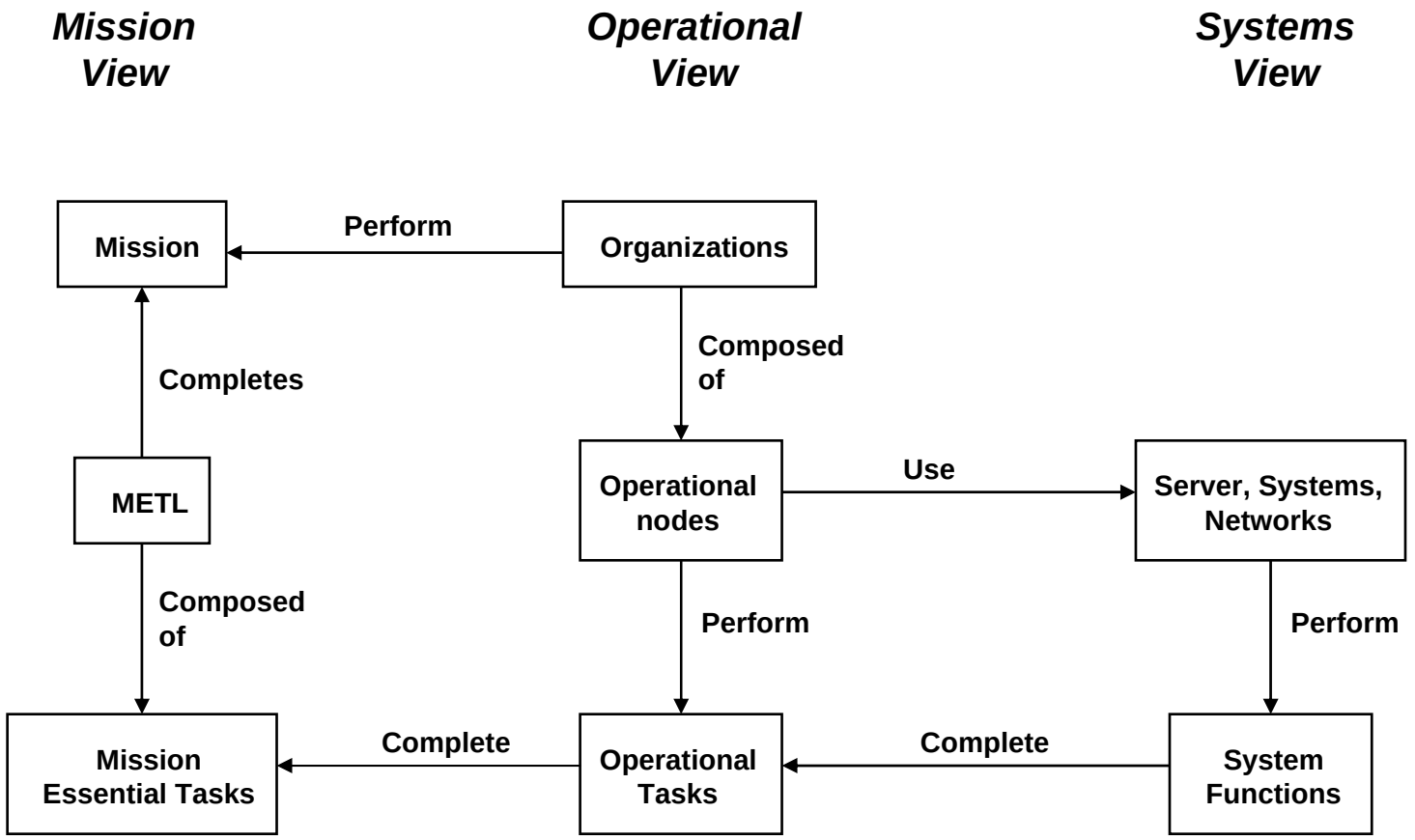
Table 6a. ATO Production Operational Tasks

Description	Operational Node	Required Inputs	Output	Mission Essential Tasks Completed
Plan and Schedule Tanker Missions	Air Refueling	MAAP, SPINS, Intel Assessment, Airlift Requirements	Tanker Schedule	OP2.1.4, OP6.1.1, ST4.3.1
Prepare MAAP Inputs	Air Refueling	Tanker Schedule	MAAP Inputs	OP2.1.4, OP6.1.1, ST4.3.1
Plan and Schedule Airlift Missions	AME	Intel Assessment, Weather Forecast, Airfield Capability Assessment, ACO and SPINS	Airlift Schedule	ST4.3.1

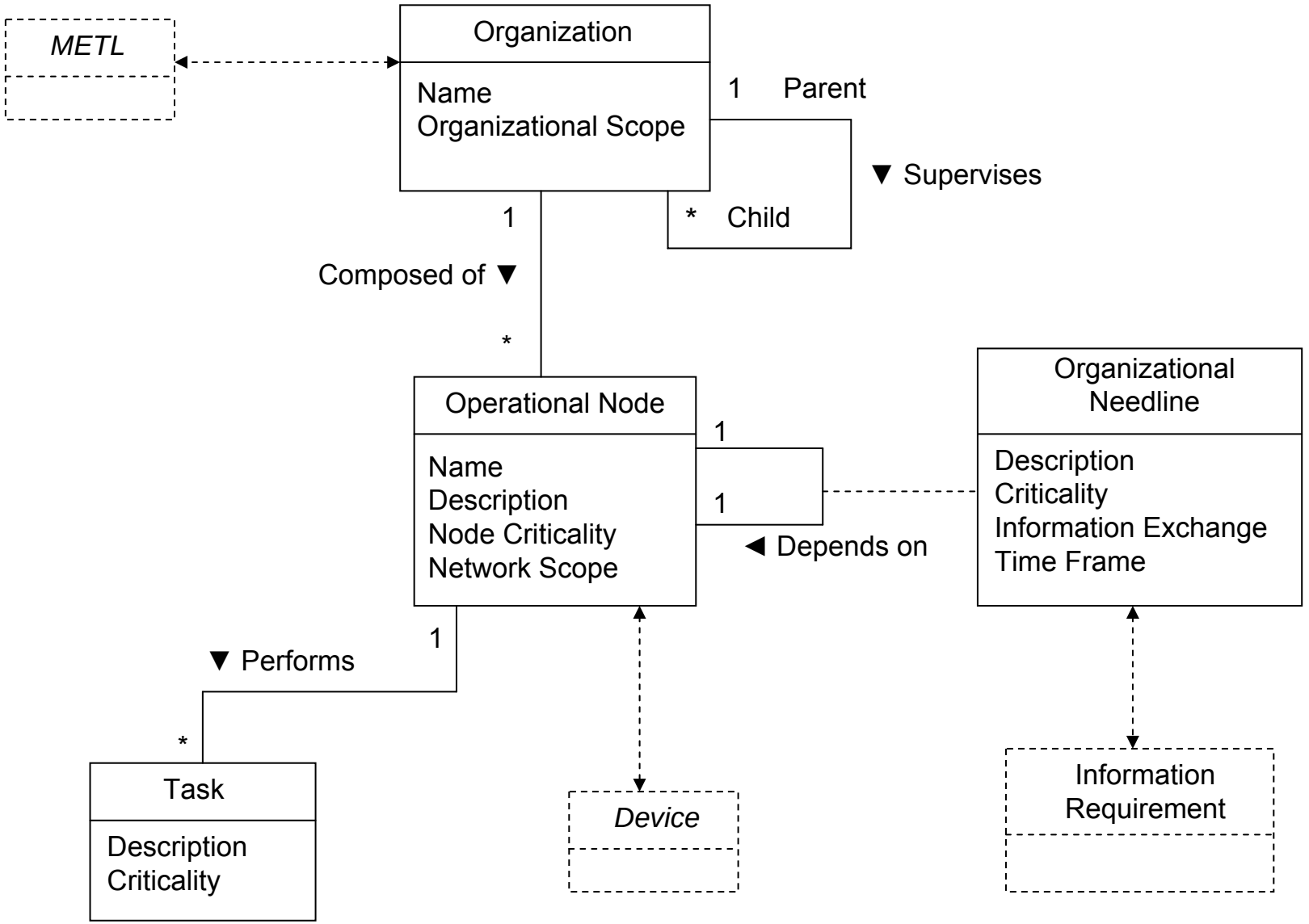
Table 12a. Operational Task/System Function Associations

Operational Task	System Functions
Plan and Schedule Tanker Missions	1. Retrieve Airlift Requirements 2. Plan Tanker Missions 3. Schedule Tanker Missions
Prepare MAAP Inputs (Air Refueling)	1. Retrieve Airlift Requirements 2. Plan Tanker Missions 3. Generate Component MAAP Inputs
Plan and Schedule Airlift Missions	1. Generate Weather Forecast 2. Retrieve Strategic Mobility Information 3. Schedule Airlift Missions

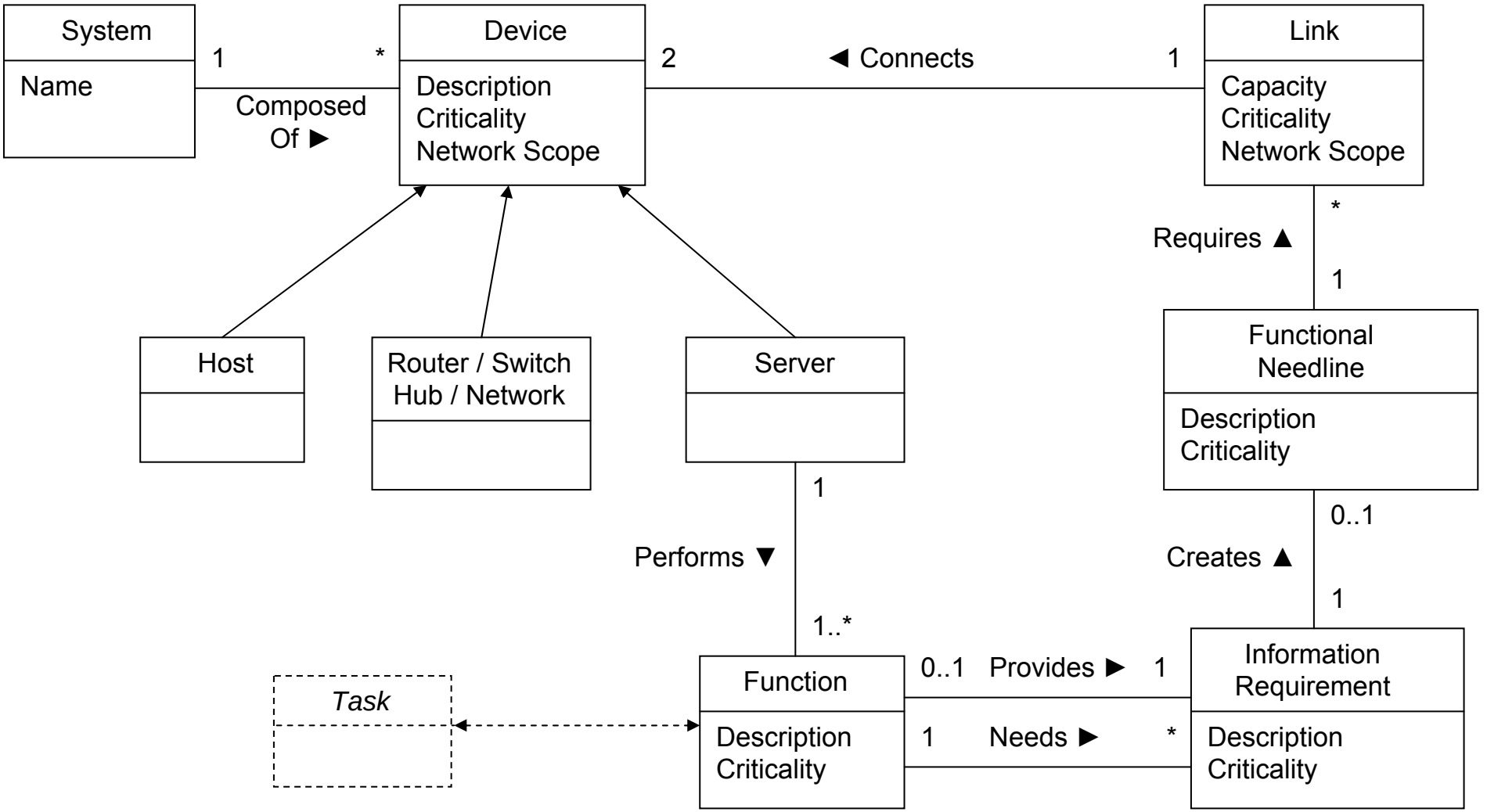
Multi-Layer Model Problem Domain



OV Layer

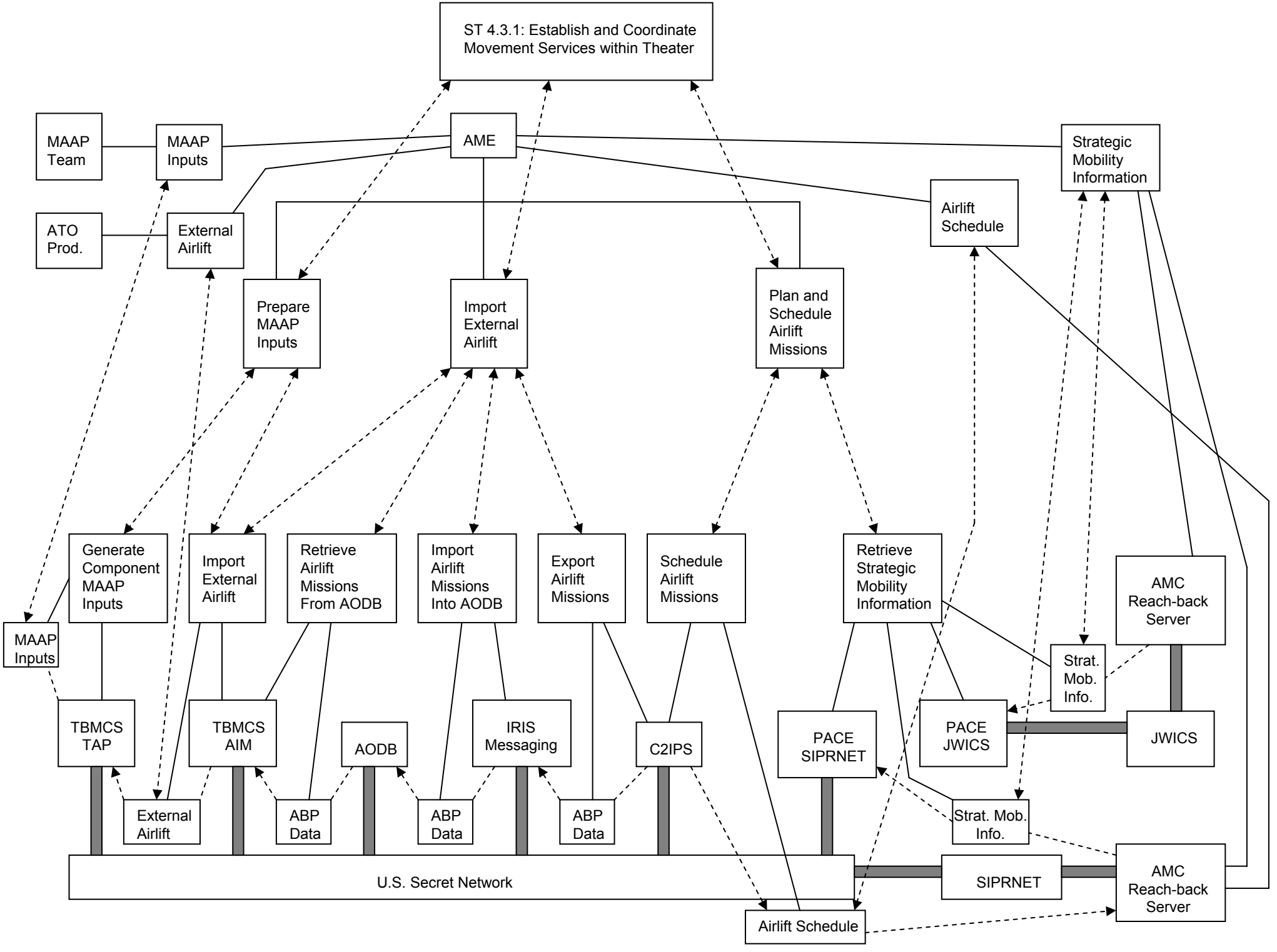

METL
Organization
Name
Organizational Scope
1 Parent
▼ Supervises
1
* Child
Composed of ▼
*
Operational Node
Name
Description
Node Criticality
Network Scope
1
1
◄ Depends on
Organizational Needline
Description
Criticality
Information Exchange
Time Frame
1
▼ Performs
*
Task
Description
Criticality
Device
Information Requirement

SV Layer


System
Name
1
*
Composed Of ▶
Device
Description
Criticality
Network Scope
2
◀ Connects
1
Link
Capacity
Criticality
Network Scope
*
Requires ▲
1
Functional Needline
Description
Criticality
0..1
Creates ▲
1
Host
Router / Switch
Hub / Network
Server
1
Performs ▼
1..*
Task
Function
Description
Criticality
0..1
Provides ▶
1
1
Needs ▶
*
Information Requirement
Description
Criticality

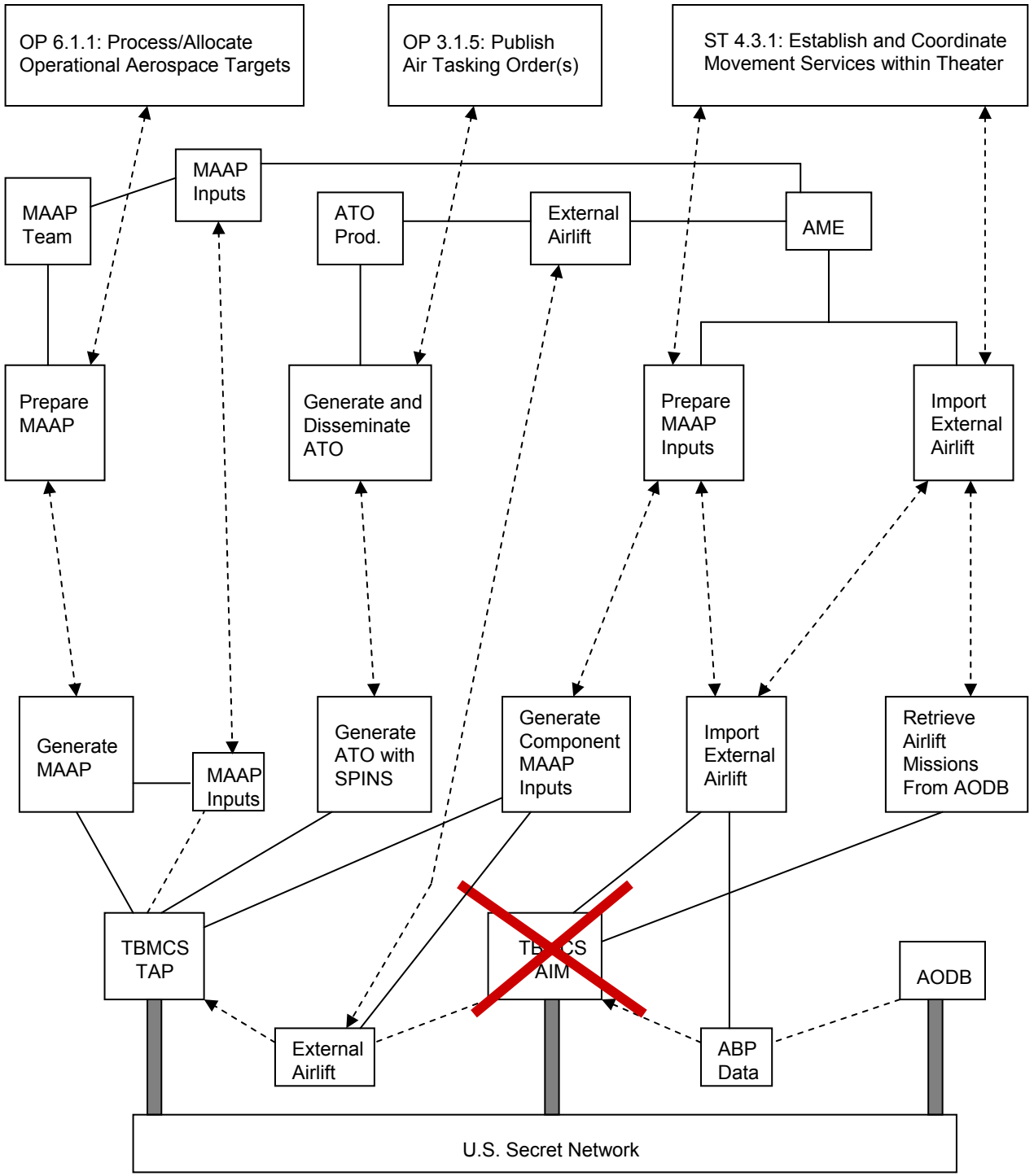
Top-Down Analysis

- Starts at the mission layer
- Identifies all operational tasks and system functions that help complete a mission essential task
- Supporting operational nodes, systems, and networks are also identified


ST 4.3.1: Establish and Coordinate Movement Services within Theater
MAAP Team
MAAP Inputs
AME
Strategic Mobility Information
ATO Prod.
External Airlift
Airlift Schedule
Prepare MAAP Inputs
Import External Airlift
Plan and Schedule Airlift Missions
Generate Component MAAP Inputs
Import External Airlift
Retrieve Airlift Missions From AODB
Import Airlift Missions Into AODB
Export Airlift Missions
Schedule Airlift Missions
Retrieve Strategic Mobility Information
AMC Reach-back Server
MAAP Inputs
Strat. Mob. Info.
TBMCS TAP
TBMCS AIM
AODB
IRIS Messaging
C2IPS
PACE SIPRNET
PACE JWICS
JWICS
External Airlift
ABP Data
ABP Data
ABP Data
Strat. Mob. Info.
U.S. Secret Network
SIPRNET
AMC Reach-back Server
Airlift Schedule

Bottom-up Analysis

- Starts at a network device (server, router, etc.)
- Identifies affected system functions (either on server or receive inputs from server)
- Affected operational and mission essential tasks can then be identified


OP 6.1.1: Process/Allocate Operational Aerospace Targets
OP 3.1.5: Publish Air Tasking Order(s)
ST 4.3.1: Establish and Coordinate Movement Services within Theater
MAAP Inputs
MAAP Team
ATO Prod.
External Airlift
AME
Prepare MAAP
Generate and Disseminate ATO
Prepare MAAP Inputs
Import External Airlift
Generate MAAP
MAAP Inputs
Generate ATO with SPINS
Generate Component MAAP Inputs
Import External Airlift
Retrieve Airlift Missions From AODB
TBMCS TAP
TBMCS AIM
AODB
External Airlift
ABP Data
U.S. Secret Network

Results

- Mission impact of network and system outages clearly demonstrated
  - All operational nodes, systems, tasks, and functions clearly identified
  - Operational and mission essential tasks affected by an outage completely identified
- Traceability through all layers of the model
- Usable for top-down and bottom-up analysis
- General methodology with broad applicability

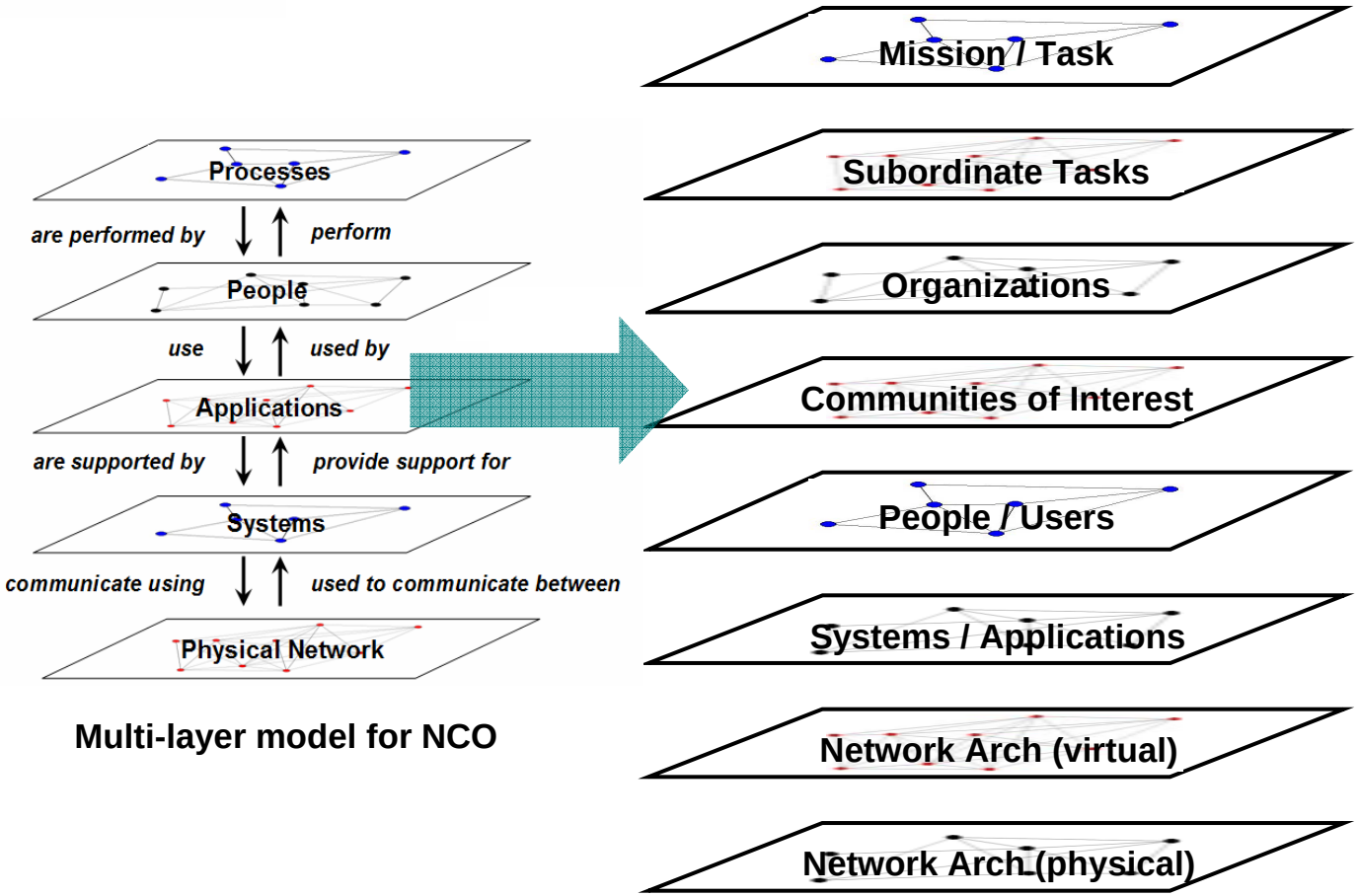
Areas for Future Research

- Automating data input…cannot rely on manual inputs
  - Self-awareness
- How to handle degradation?
  - Network connectivity degradation, but services are available locally
  - Specific service may be down, but the network is green
- Determining Resource Criticality
  - Different users, different times, different priorities
  - Weighting and probabilities of degradation / destruction
- New Architectures
  - Modeling Network Virtualization
  - Service Oriented Architectures
- Cyberspace situational awareness

Map & Mission Context

- What does cyberspace “look like”
  - Common Operational Picture
  - Traceability to real world missions
- Cyberspace changes depending on how you look at it
  - Is multi-dimensional…has many aspects
  - Is a medium of operations (like air, land, and sea)
  - Supports operations in the physical domain (air, land, sea)
- Cyberspace is all about collecting, processing, and exchange of information
  - Has various layers of abstraction…just like information
  - The value / nature of information depends on where you sit and why you need it

Cyberspace Situational Awareness



Multi-layer model for NCO

Depending on your function, your desired "map" of cyberspace (i.e., what you care about) is different

- ***Cyberspace as domain of ops*** **(attack/defend) – each layer is an avenue for attack and we need to understand linkages for targeting, damage assessment, etc.**
- ***Cyberspace as supporting infrastructure*** **– need clear mapping of cyber assets to physical world missions, tasks, organizations, etc.**

Questions?